

The Botnet is Back: SSC STRIKE Team Uncovers a Renewed Cyber Threat

 securityscorecard.com/blog/botnet-is-back-ssc-strike-team-uncovers-a-renewed-cyber-threat/



A silent danger is sweeping through the world's critical infrastructure. The SecurityScorecard STRIKE Team has uncovered a resurgence of Volt Typhoon—a state-sponsored cyber-espionage group from the Asia-Pacific region, known for its precision and persistence. This is no ordinary attack. Volt Typhoon exploits unprotected, outdated edge devices within targeted critical infrastructure.

Renewed Threat to Governments and Critical Infrastructure: Volt Typhoon is Back

Once thought dismantled, Volt Typhoon has returned, more sophisticated and determined than ever. Unlike attackers who vanish when discovered, this adversary digs in even deeper when exposed. According to the STRIKE Team, Volt Typhoon's tactics are adaptive and multifaceted. They exploit legacy weaknesses in Cisco RV320/325 routers and Netgear

ProSafe routers, devices long past their prime, using them as operational relay boxes. These end-of-life devices become perfect entry points, and in just 37 days, Volt Typhoon compromised 30% of visible Cisco RV320/325 routers.

These compromised routers form a covert transfer network that keeps the botnet's presence hidden. Every layer of Volt Typhoon's infrastructure is designed to blend malicious activities into everyday operations, making them difficult to detect and even harder to remove—especially in sectors like governments and critical infrastructure that still depend on outdated technology.

Botnet Rebuilds Using Old Infrastructure

Volt Typhoon's evolving attacks over recent years illustrate a persistent threat that continues to grow, even under observation.

- **2019:** Security researchers uncover vulnerabilities in Cisco routers, leaving the devices exposed. Industries like energy, dependent on legacy infrastructure, become prime targets.
- **Late 2023:** Volt Typhoon reappears, launching its JDYFJ botnet, a network of compromised Cisco and Netgear routers identified by a self-signed SSL certificate named JDYFJ. This botnet leverages C2s in the Netherlands, Latvia, and Germany to mask traffic, creating encrypted channels that evade tracking.
- **October 2023:** Volt Typhoon embeds a compromised VPN device in New Caledonia, creating a covert bridge between Asia-Pacific and the Americas. This bridge keeps their network alive, hidden from standard detection.
- **Early 2024:** Global law enforcement disrupts parts of the botnet. Volt Typhoon quickly sets up new command servers on Digital Ocean, Quadranet, and Vultr, registering fresh SSL certificates to evade authorities.
- **September 2024:** The botnet persists, using the JDYFJ cluster to route traffic covertly worldwide. Connections from New Caledonia and router nodes remain active for over a month, reinforcing Volt Typhoon's infrastructure.

Volt Typhoon's Global Network Expands

The STRIKE Team's deep investigation has exposed Volt Typhoon's complex network built on compromised SOHO (small office/home office) and EOL (end-of-life) devices. This group has weaponized outdated routers on a global scale, weaving layers of obfuscation that mask their presence and make detection exceptionally difficult.

These compromised routers act as digital chameleons, facilitating the covert movement of data while mimicking normal network traffic. Analysts have identified MIPS-based malware on these devices, similar to Mirai, engineered to establish covert connections and

communicate via port forwarding over 8443. This method keeps Volt Typhoon's command operations off the radar, even for seasoned cybersecurity teams.

Webshells, such as *fy.sh*, are strategically implanted in routers, allowing Volt Typhoon to maintain persistent access and secure remote control. The attack doesn't just hide—it integrates seamlessly into routine network operations. The result? A resilient foothold, particularly within governmental and critical infrastructure sectors, that camouflages malicious activities and complicates any cleanup efforts.

An Island Hub for Cyber Espionage

New Caledonia is crucial to Volt Typhoon's global operations. A compromised VPN device on this small Pacific island acts as a silent bridge, routing traffic between Asia-Pacific and American regions without detection. This covert hub enables Volt Typhoon to avoid scrutiny and extends the botnet's reach.

Supply Chain Weakness Creates Cyber Risk

Critical infrastructure presents an attractive target for state-sponsored attackers due to its essential role in economic stability. For example, disrupting an energy grid doesn't merely cause power outages—it raises energy prices, impacts industries globally, and destabilizes economies. A dependence on legacy technology, combined with vulnerable third-party vendors, creates a perfect storm for exploitation. The STRIKE Team's findings confirm that many third-party vendors lack robust defenses, offering easy entry points that Volt Typhoon—and others—can exploit.

Is Ransomware Funding These Threats?

Though Volt Typhoon doesn't directly deploy ransomware, it operates within an ecosystem transformed by Ransomware-as-a-Service (RaaS). Under this model, cybercriminals reinvest ransom payments into more sophisticated tools, making their efforts even more dangerous. Reliance on third-party vendors and cloud providers heightens this risk, as ransom-funded advancements in hacking fuels new waves of attacks. This creates a dangerous cycle for an already vulnerable industry.

AI-Powered Attacks Increase Cyber Risks in Energy

The SecurityScorecard and KPMG report, "[*Third-Party Breaches are the Top Threat for the U.S. Energy Sector*](#)," reveals rising cyber threats in the U.S. energy industry. Third-party breaches account for 45% of incidents. The report highlights risks from state-sponsored attacks like those by Volt Typhoon. This raises concerns that AI-powered methods could intensify these threats. AI could make future attacks more precise and harder to detect. The report emphasizes the urgent need for strong cybersecurity across the energy supply chain.

A Global Stand Begins

In 2023, 68 nations, led by the United States, launched the International Counter-Ransomware Initiative. This coalition aims to reduce the need for ransom payments, offering financial and technical recovery support. Simultaneously, the G7 committed to bolstering supply chain security, especially for critical sectors like energy. Together, these efforts lay the groundwork to counter ransomware-driven threats and protect essential infrastructure.

Volt Typhoon is a Wake-Up Call for Infrastructure Security

The STRIKE Team's discoveries highlight the expanding threat posed by Volt Typhoon. As the botnet spreads and its tactics deepen, governments and corporations must urgently address weaknesses in legacy systems, public cloud infrastructures, and third-party networks. Volt Typhoon is both a resilient botnet—and a warning. Without decisive action, this silent threat could trigger a critical infrastructure crisis driven by vulnerabilities left unresolved.

SecurityScorecard's STRIKE Team

SecurityScorecard's STRIKE Team has access to one of the world's largest databases of cybersecurity signals, dedicated to identifying threats that evade conventional defenses. With proactive risk management and a rapid response approach, SecurityScorecard offers companies protection against third-party risks and the ability to counter active threats like Volt Typhoon.

Discover how SecurityScorecard and its STRIKE Team can strengthen your enterprise's security. [Learn more here](#).

For media inquiries, please contact us at [\[email protected\]](#).